Rodrigo Méndez-Ramírez, Adrian Arellano-Delgado, César Cruz-Hernández, Fausto Abundiz-Pérez, Rigoberto Martínez-Clark, 2018. Chaotic digital cryptosystem using serial peripheral interface protocol and its dsPIC implementation. *Frontiers of Information Technology & Electronic Engineering*, 19(2):165-179. https://doi.org/10.1631/FITEE.1601346

Chaotic digital cryptosystem using serial peripheral interface protocol and its dsPIC implementation

Key words: Chaotic systems; Statistical tests; Embedded systems; dsPIC microcontroller; Serial peripheral interface (SPI) protocol

Corresponding author: César CRUZ-HERNÁNDEZ
E-mail: ccruz@cicese.mx
ORCID: http://orcid.org/0000-0002-2593-8658

Motivation

1. Current massive use of digital communications demands a secure link by using an embedded system (ES) with data encryption in the protocol level. The serial peripheral interface (SPI) protocol is commonly used by manufacturers of ESs and integrated circuits for applications in areas such as wired and wireless communications.

2. We propose the chaos implementation in ES of a digital cryptosystem using the SPI protocol. The digital-to-analog converter process is used to acquire and reconstruct confidential messages in digital signal processing applications.

Main idea

1. Design and experimental implementation of a chaotic encryption and decryption algorithm applied to the SPI communication protocol is presented. The SPI protocol is configured in 16-bits to synchronize the transmitter and the receiver considering a symmetric key. The design of the chaotic encryption algorithm along with its counterpart in the decryption is based on the chaotic Hénon map and two methods for blur and permute (in combination with DNA sequences).

2. Security of the cryptogram is tested by a statistical analysis. The digital processing capacity of the proposed algorithm is implemented in dsPIC microcontrollers.

Main idea (Cont'd)

Design and experimental implementation of the digital cryptosystem based in chaos using SPI protocol

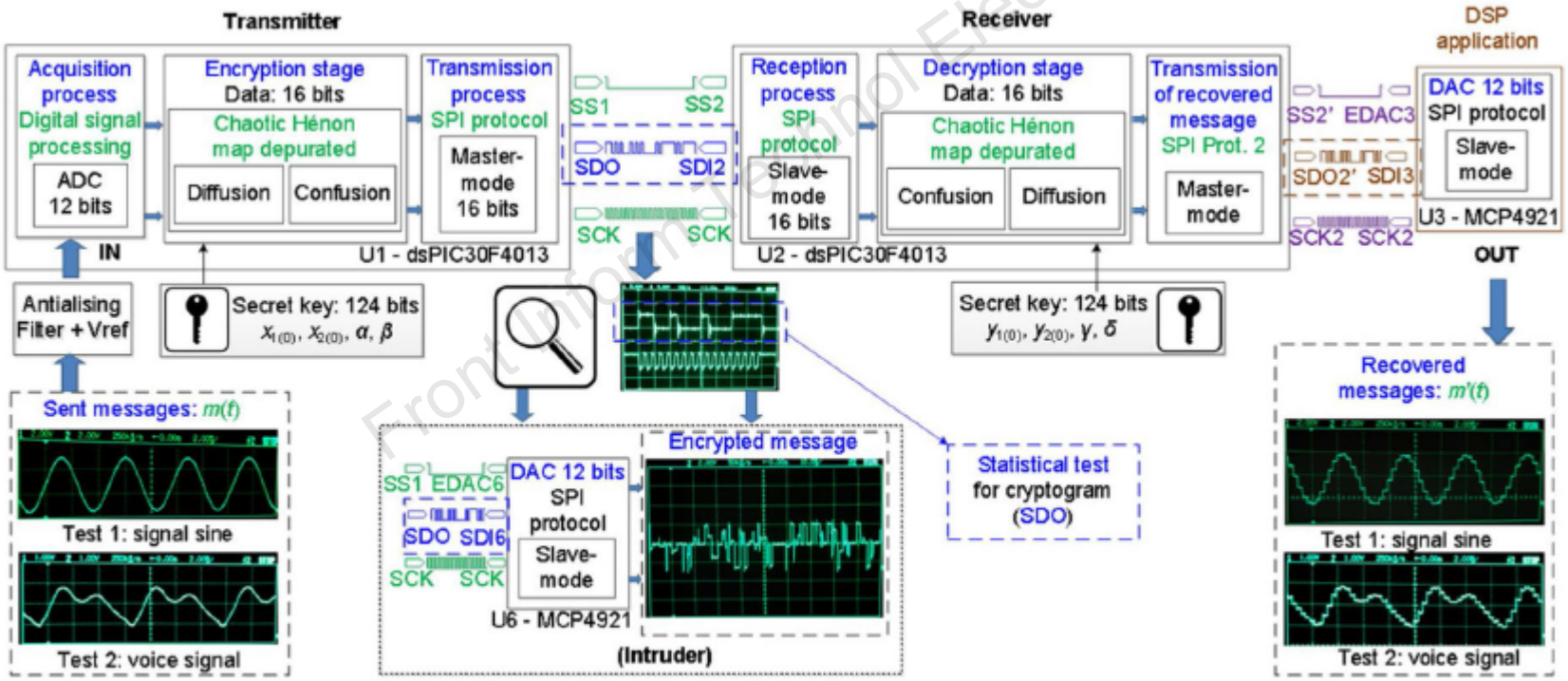


Fig. 1 Block diagram of the embedded cryptosystem (references to color refer to the online version of this figure)

Method

1. Design and experimental implementation of the digital cryptosystem based in chaos.
2. We describe the statistical tests to prove the hypothesis that messages are secures from the observer standpoint. To show whether the proposed algorithm reproduces PR sequences, we perform the statistical tests to the cryptogram.
3. The time complexity of the proposed algorithms of the digital cryptosystem are implemented in dsPICs.
4. Three experimental tests are conducted to probe the performance of the digital cryptosystem: sensitivity of secret keys, sine signal as message, and voice message.

Major results

Test 1: sensitivity of secret keys

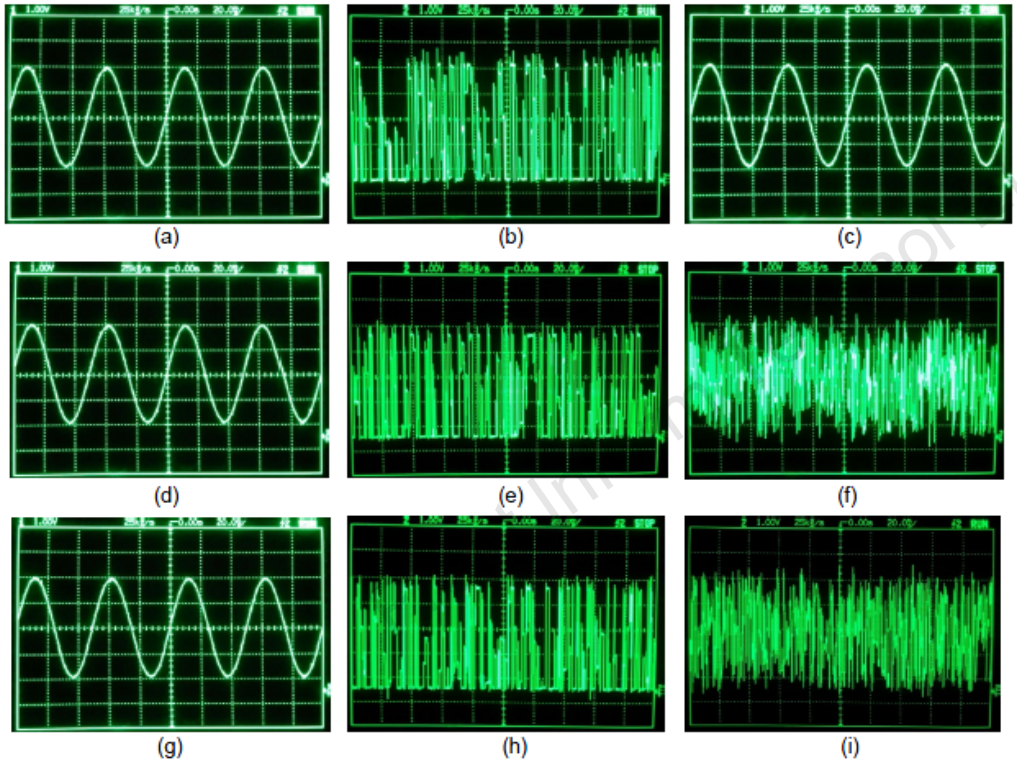


Fig. 10 Results of sensitivity tests of secret keys on an ES with case 1: original $m_1(t)$ (a), cryptogram (b), and reception of $m_1'(t)$ (c); case 2: original $m_1(t)$ (d), cryptogram (e), and reception of $m_1'(t)$ (f); and case 3: original $m_1(t)$ (g), cryptogram (h), and reception of $m_1'(t)$ (i)

Table 9 Sensitivity test of secret keys on ES

Case	Secret key on U1	Secret key on U2
1	K_1	K_1
2	K_1	K_2
3	K_1	K_3

Major results (Cont'd)

Test 2: sine signal as message

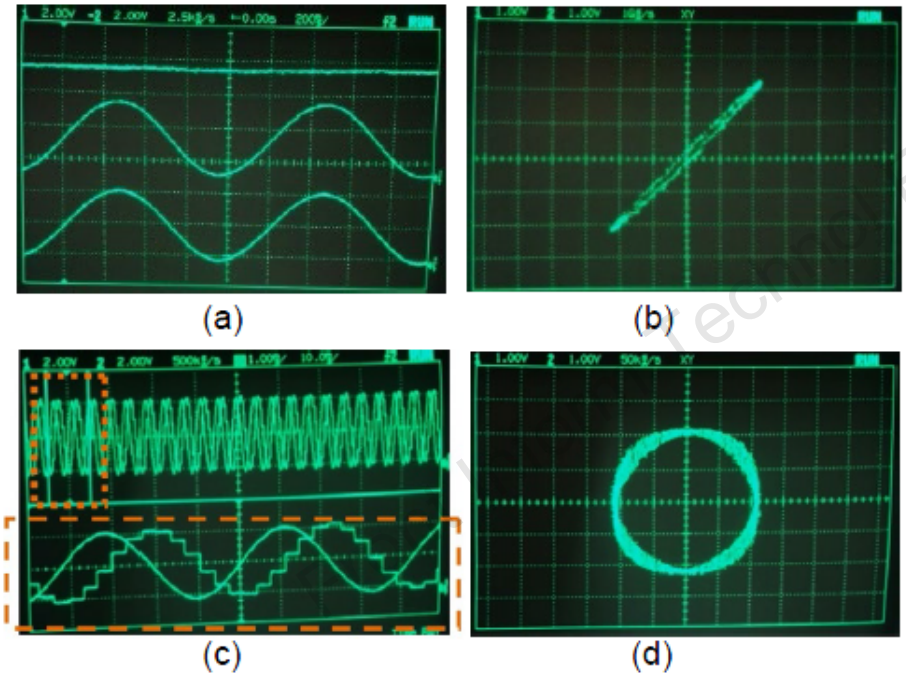
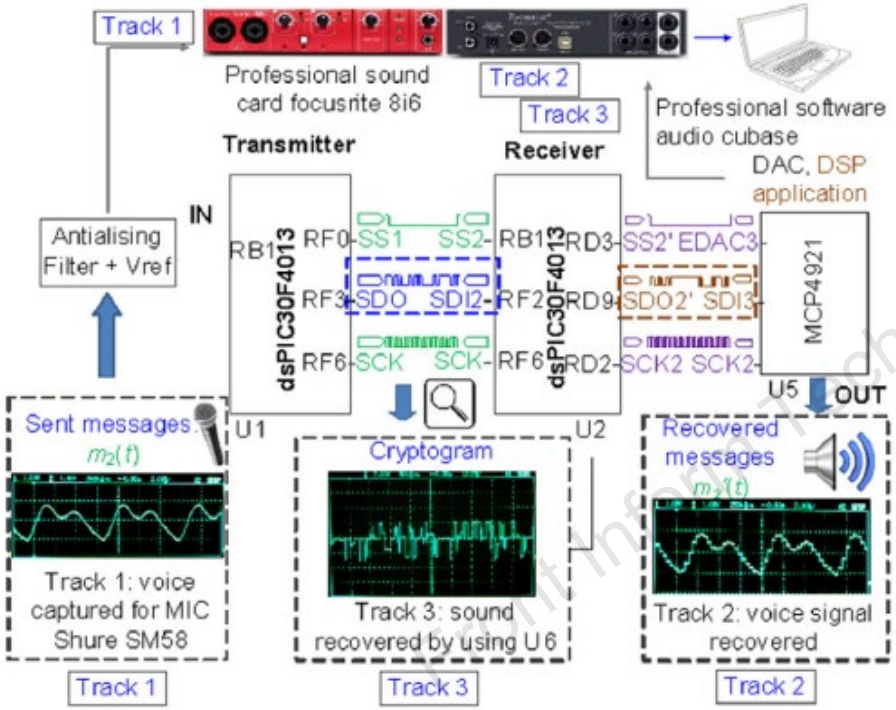


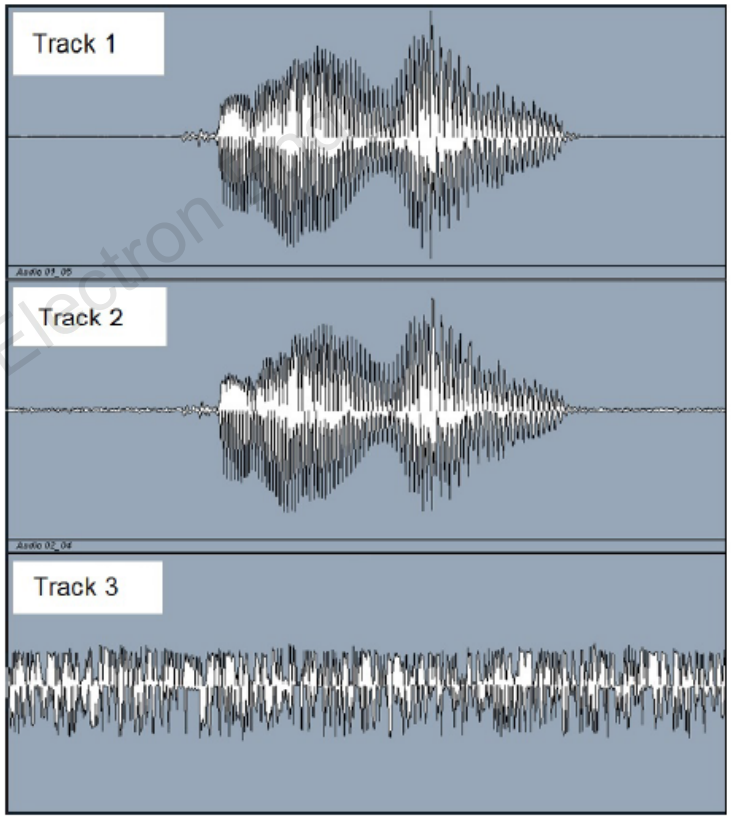
Fig. 11 Test results using the sine signal message (Eq. (24)): (a) $m_1(t)$, $m_1'(t)$, and error message $e_1(t)$; (b) phase plane $m_1(t)$ vs. $m_1'(t)$ with f=10 Hz; (c) zoom of messages $m_1(t)$ and $m_1'(t)$; (d) phase plane $m_1(t)$ vs. $m_1'(t)$ with f=210 Hz and $\theta=\pi/2$

Major results (Cont'd)

Test 3: voice message



(a)



(b)

Fig. 12 Test results on the ES using voice message: (a) ES connected with external audio devices; (b) the audio tracks with the messages recorded using software Cubase (references to color refer to the online version of this figure)

Conclusions

1. We have presented the design and implementation of a chaotic encryption algorithm using the communication protocol SPI 16-bits microcontrollers on dsPICs to acquire, process, encrypt, transmit, synchronize, receive, decrypt, and re-transmit messages using an external DAC with DSP theory.

2. The cryptogram has good performance for generating PR sequences. This algorithm can be used in ICs with the standard SPI protocol.

3. The quality of the recovered message depends on the processing capacity of the ICs. The ES is easy to be in-stalled on a protoboard due to its dual-in-line-package (DIP) and has a low-cost implementation because the system cost less than 30 USD.